National Security Agency/Central Security Service

INFORMATION ASSURANCE DIRECTORATE

CGS Threat Assessment Capability

Version 1.1.1

The Threat Assessment Capability identifies, analyzes, and prioritizes threat information by identifying threats and threat sources, understanding the threat's capability, and determining the likelihood of the threat occurring.

07/30/2012

CGS Threat Assessment Capability

Version 1.1.1

Table of Contents

1 Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1

2 Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

The Threat Assessment Capability identifies, analyzes, and prioritizes threat information by identifying threats and threat sources, understanding the threat's capability, and determining the likelihood of the threat occurring.
A threat is the potential for a particular threat source (or set of threat sources) to successfully exploit a particular vulnerability (or set of vulnerabilities) that has the potential to adversely impact agency, agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

A threat source is either 1) the intent and method targeted to intentionally exploit a particular vulnerability (or set of vulnerabilities) or 2) a situation and method that may accidentally overwhelm a vulnerability (or set of vulnerabilities). Common threat sources include, but are not limited to, natural threats such as floods, earthquakes, and tornadoes; human threats such as terrorists, computer criminals, and insiders; and environmental threats such as long-term power failure, chemicals, and pollution.

A threat capability is the level of access, resources, knowledge, and skill that a threat source is capable of applying against technical, personnel, physical, and environmental aspects of the Enterprise. The threat likelihood is the probability of a given threat source's attempt to exploit a given vulnerability.

3 Capability Gold Standard Guidance

The Capability Gold Standard Guidance evaluates the Enterprise needs and overlays the expected Gold Standard behavior. The guidance goes beyond the concept of "good enough" when describing the Gold Standard recommendations, considers industry best practices, and describes a level of security that not only meets current standards but also exceeds them across the Enterprise.

The Threat Assessment Capability works closely with the Vulnerability Assessment Capability to enable proper threat identification, analysis, prioritization, and sharing of information. Enterprises shall know their vulnerabilities and leverage this information to

identify specific threats and determine their impacts and risks, as well as understand new vulnerabilities that exist based on analysis of an identified threat.

The Threat Assessment Capability shall consist of a full spectrum threat source and threat capability analysis of attacks against technical, personnel, physical, and environmental aspects of the Enterprise, including supply chain, close access technical attacks, and insider threats. The Enterprise shall leverage all Community resources, including resources in the broader intelligence and law enforcement community, to develop threat information as it specifically applies to technical, personnel, physical, and environmental aspects of the Enterprise. To cover the full spectrum, the Enterprise shall tie into multiple government, civilian, and commercial sources of threat, incident, attack, information technology (IT) security, and virus scanning industries to gain insight into current and evolving cyber- and IT-related threats to create a comprehensive threat picture. Threat Assessment encompasses full spectrum threat awareness, investigations, active operations, provocations, and deception activities.

The Threat Assessment Capability shall obtain a full spectrum of input and fuse all inputs to determine relevant potential threats. There are resources for all types of threats, such as the Joint Threat Incident Database (JTID), Defense Intelligence Agency (DIA), National Security Agency (NSA), Central Intelligence Agency (CIA), Federal Bureau of Investigations (FBI), Department of Homeland Security (DHS), United States Computer Emergency Readiness Team (US-CERT), and Federal Computer Incident Response Center (FedCIRC). Sources such as JTID are populated when a threat is detected and the threat is associated with an actor. There are also resources for threat information at the local level within an Enterprise, such as the Staff Security Officer (SSO). The Enterprise shall understand how Threat Assessments are handled and what resources it can rely on internally as well as externally for Threat Assessment information. If an Enterprise relies on an external Organization, the Enterprise shall identify a subset of threats that apply to local enclaves as well as at the Enterprise level. If an Enterprise is not large or does not have the manpower to stand up its own threat Organization, a formal relationship shall be established with a set of external organizations to provide the needed threat data in the appropriate form and format. After the information is obtained, the Enterprise shall be prepared to perform further analysis on applicability to its enclave/Organization.

The Threat Assessment Capability shall provide an effective means or access to an effective means to identify, analyze, and prioritize every threat that is identified on an ongoing basis. The Threat Assessment Capability shall work with other Capabilities to

identify threats using a full range of intelligence sources. Monitoring and detection Capabilities such as Network Intrusion Detection, Host Intrusion Detection, Network Enterprise Monitoring, and Personnel Enterprise Monitoring can provide input to help the Enterprise discover threats. Raw data provided from other Capabilities requires additional analysis to ensure applicability and usefulness, and the information received contributes to overall situational awareness. Each identified threat feeds into the Risk Identification Capability and is analyzed by the Risk Analysis Capability to determine what resources it affects and its potential risk of attack and successful exploitation. The threat may then be assigned a priority from a purely threat perspective or it can be combined with additional information to be prioritized from a risk or risk mitigation cost-benefit perspective. In the case of prioritizing threats based on a risk mitigation cost-benefit perspective, rather than a threat prioritization approach, a portfolio management approach to threat and risk mitigation often provides greater total threat and risk mitigation than prioritizing just on threat or risk.

Threats shall be reported in accordance with established requirements. These reports shall be accessible to affected Organizations, as required and/or agreed upon. The Enterprise shall share threat information across boundaries with Organizations that have like or similar threats. To the greatest extent possible, appropriate Memorandums of Agreement (MOAs), contracts, or other vehicles to establish organizational cooperation shall be in place between Organizations to share this information.

The Threat Assessment Capability shall monitor threats and perform trend analysis. Trend analysis will assist in determining the intent and capabilities of the attackers.

4 Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. The Enterprise understands its mission and data flows.
2. The Enterprise understands its network boundaries.
3. The Enterprise knows the systems that reside on its networks.
4. The Enterprise knows its personnel and their associated tasks.
5. The Enterprise understands the physical characteristics of its environment, and the security level of the physical and environmental protections are defined in accordance with protection needs.

6. The Enterprise knows the value and priority of its assets.

5 Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

1. The Capability identifies and characterizes potential threats to the technical, personnel, physical, and environmental aspects of the Enterprise.
2. The Capability analyzes and prioritizes threats based on the specific Organization.
3. The Capability reports its findings to the cognizant security authority and other affected Organizations as required.
4. The Capability informs risk management processes.

6 Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the Organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

When Threat Assessments are performed correctly, the Organization will possess a capability to identify information about potential threats, assess applicability of those potential threats, prioritize threat information, and inform appropriate security personnel and affected Organizations. Selecting appropriate threat information resources is an important part of the threat identification and characterization process. No one information source contains all relevant threat information. The Organization will ensure access to applicable Community resources is in place to ensure a full spectrum threat analysis occurs.

The Threat Assessment Capability provides information to the Signature Repository Capability, which is a centrally managed signature repository for network security tools such as anti-virus updates, network sensors, and other information assurance (IA) applications. The signatures define known attack patterns and will be used by the Organization to understand attack patterns and their relationship to specific threats. The threat signatures are also employed in various real-time monitoring activities.

The Threat Assessment Capability will be highly automated. Determination processes are routinely documented and codified as rules that can be acted upon when thresholds of interest are reached within a system or as a result of a particular process, and where there is little ambiguity and uncertainty associated with the nature and characterization of the threat. As rules are established, the Organization will make them a part of the automated set executed routinely by the Detection and Incident Response Capabilities. New threats, which have yet to be properly characterized, can then be discovered and examined.

All external sources with agreements in place make available any raw data, observations, or derived insight. When receiving raw data from external sources, the Organization will identify a subset of threats that apply to it at the local enclave level as well as at the Enterprise level. In addition, instances may occur where the threat data is provided within the Organization, and the Threat Assessment will need to be manual. Monitoring and Detection Capabilities will make available raw data to help the Organization discover threats. Raw data provided from external sources, as well as from the Organization's local Capabilities, will require additional analysis by the Organization to ensure applicability and usefulness. This information will contribute to overall situational awareness. The Organization will perform a detailed analysis on all available threat data, generating a threat picture and informing all affected Organizations. Based on the information made available for each identified threat, the data will be trended by the Organization to determine the characteristics of the actor or group of actors behind the threat. Over time, profiles for the actors will be generated. Such profiles will be used to determine the threat capability, intent, and Organization's ability to defend against the threat, thus preventing an adversary from using and exploiting a vulnerability.

The Organization will assign a priority to each threat, which is a factor of the likelihood of attack (risk) and the value of the information at risk. This priority is important because it allows remediation teams to focus on the more critical threats first. The Organization will establish an automated process set up for monitoring ongoing threats. Over time, threats may vary in severity or even go away. When the Threat Assessment Capability is implemented correctly, the Organization will possess a Capability that manages the entire lifecycle of a threat from identification to communication to the Manage Risk Capabilities. Different systems, networks, agencies, or departments will require a different scope of assessment, depending on the technology, personnel, physical, and environmental aspects implemented within their Enterprise and the importance of their missions. Threats will be identified by deliberate action of this Capability or reported by

the actions of another Capability. Either way, each new threat will be documented and analyzed individually by appropriate security personnel within the Organization.

The Organization will leverage observations and derived insights to help form a view that may be used to determine the aggregate threat and maintain the security posture. In addition to fully documenting each threat in each step of the assessment, periodic or ad hoc reports will be generated by the Organization based on operational drivers to keep appropriate security personnel and affected Organizations updated on the status of important threats and to suggest recommended courses of action. The Organization will share threat information across boundaries with connected Organizations, as required or agreed upon. As truly severe threats are uncovered, alerts will be sent as well.

The Organization will monitor evolving threats over time and analyze any trends that have been developed. If possible, threats will be grouped into categories to further refine the rules used in processes. Source data also will be trended and attacker profiles generated where possible. These profiles will be used to determine capabilities and intent of the attackers, and recommendations will be made about existing policies or implementations that should be changed.

7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate with or influence one another.

7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.

- Network Mapping–The Threat Assessment Capability relies on the Network Mapping Capability to provide an understanding of what is in the Enterprise, which is key to assessing the Organization’s susceptibility to threats.
- Network Boundary and Interfaces–The Threat Assessment Capability relies on the Network Boundary and Interfaces Capability to provide an understanding of what is in the Enterprise, which is key to assessing the Organization’s susceptibility to threats.

- Utilization and Performance Management–The Threat Assessment Capability relies on the Utilization and Performance Management Capability to provide an understanding of what is in the Enterprise, which is key to assessing the Organization's susceptibility to threats.
- Understand Mission Flows–The Threat Assessment Capability relies on the Understand Mission Flows Capability to provide an understanding of what is in the Enterprise, which is key to assessing the Organization's susceptibility to threats.
- Understand Data Flows–The Threat Assessment Capability relies on the Understand Data Flows Capability to provide an understanding of what is in the Enterprise, which is key to assessing the Organization's susceptibility to threats.
- Hardware Device Inventory–The Threat Assessment Capability relies on the Hardware Device Inventory Capability to provide an understanding of what is in the Enterprise, which is key to assessing the Organization's susceptibility to threats.
- Software Inventory–The Threat Assessment Capability relies on the Software Inventory Capability to provide an understanding of what is in the Enterprise, which is key to assessing the Organization's susceptibility to threats.
- Understand the Physical Environment–The Threat Assessment Capability relies on the Understand the Physical Environment Capability to provide an understanding of what is in the Enterprise, which is key to assessing the Organization's susceptibility to threats.
- Vulnerability Assessment–The Threat Assessment Capability relies on the Vulnerability Assessment Capability to feed prioritized vulnerability alerts about vulnerabilities that may be exploitable by known threat actors.
- Network Enterprise Monitoring–The Threat Assessment Capability relies on the Network Enterprise Monitoring Capability to provide information to help discover threats.
- Physical Enterprise Monitoring–The Threat Assessment Capability relies on the Physical Enterprise Monitoring Capability to provide information to help discover threats.
- Personnel Enterprise Monitoring–The Threat Assessment Capability relies on the Personnel Enterprise Monitoring Capability to provide information to help discover threats.
- Network Intrusion Detection–The Threat Assessment Capability relies on the Network Intrusion Detection Capability to provide information to help discover threats.

- Host Intrusion Detection–The Threat Assessment Capability relies on the Host Intrusion Detection Capability to provide information to help discover threats.
- Network Hunting–The Threat Assessment Capability relies on the Network Hunting Capability to provide information to help discover threats.
- Physical Hunting–The Threat Assessment Capability relies on the Physical Hunting Capability to provide information to help discover threats.
- Enterprise Audit Management–The Threat Assessment Capability relies on the Enterprise Audit Management Capability to provide information to help discover threats.
- Incident Analysis–The Threat Assessment Capability relies on the Incident Analysis Capability to provide information about the root cause of an incident so that a decision can be made about whether the incident presents a threat for the Enterprise. The Threat Assessment Capability also relies on the Incident Analysis Capability to provide information used to measure the effectiveness of its assessment decisions.

7.2 Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- Portfolio Management–The Threat Assessment Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Policies, Procedures, and Standards–The Threat Assessment Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.
- IA Awareness–The Threat Assessment Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training–The Threat Assessment Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities–The Threat Assessment Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.

7.3 Supporting Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are not necessary for the Capability to operate, although they support the operation of the Capability in this document.

- Network Boundary Protection–The Threat Assessment Capability relies on the Network Boundary Protection Capability to enable and protect the sharing of threat information across domain boundaries.
- Incident Response–The Threat Assessment Capability relies on the Incident Response Capability to provide information for situational awareness.

8 Security Controls

This section provides a mapping of the Capability to the appropriate controls. The controls and their enhancements are granularly mapped according to their applicability. In some instances, a control may map to multiple Capabilities.

Control Number/Title	Related Text
NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*	
AT-5 *CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS*	Control: The organization establishes and institutionalizes contact with selected groups and associations within the security community: - To facilitate ongoing security education and training for organizational personnel; - To stay up to date with the latest recommended security practices, techniques, and technologies; and - To share current security-related information including threats, vulnerabilities, and incidents. (Note: Such contacts help in determining the existing and new threats, vulnerabilities and at the end the risks) Enhancement/s: None Specified
CA-2 *SECURITY ASSESSMENTS*	Control: The organization: a. Develops a security assessment plan that describes the scope of the assessment including: - Security controls and control enhancements under assessment; - Assessment procedures to be used to determine security control effectiveness; and

	- Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative. Enhancement/s: (1) The organization employs an independent assessor or assessment team to conduct an assessment of the security controls in the information system. (2) The organization includes as part of security control assessments, [Assignment: organization-defined frequency], [Selection: announced; unannounced], [Selection: in-depth monitoring; malicious user testing; penetration testing; red team exercises; [Assignment: organization-defined other forms of security testing]].
CA-7 *CONTINUOUS MONITORING*	Control: The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes: b. A determination of the security impact of changes to the information system and environment of operation; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and d. Reporting the security state of the information system to appropriate organizational officials [Assignment: organization-defined frequency]. Enhancement/s: (1) The organization employs an independent assessor or assessment team to monitor the security controls in the information system on an ongoing basis. (2) The organization plans, schedules, and conducts assessments [Assignment: organization-defined frequency],

	[Selection: announced; unannounced], [Selection: in-depth monitoring; malicious user testing;
RA-3 *RISK ASSESSMENT*	Control: The organization: a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits; Enhancement/s: None
SA-12 *SUPPLY CHAIN PROTECTION*	Control: The organization protects against supply chain threats by employing: [Assignment: organization-defined list of measures to protect against supply chain threats] as part of a comprehensive, defense-in-breadth information security strategy. Enhancement/s: (2) The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire information system hardware, software, firmware, or services.
SA-13 *TRUSTWORTHINESS*	Control: The organization requires that the information system meets [Assignment: organization-defined level of trustworthiness]. Enhancement/s: None Specified

9 Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

Threat Assessment Directives and Policies

Title, Date, Status	**Excerpt / Summary**
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23	Summary: National Security Presidential Directive-

Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	
DoDI 3020.45 Defense Critical Infrastructure Program (DCIP) Management, 21 April 2008, Unclassified	Summary: This instruction establishes a requirement for multidisciplinary Threat Assessments related to the Defense Critical infrastructure Program (DCIP).
DoDI 4630.8 Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 30 June 2004, Unclassified	Summary: This instruction establishes a responsibility for threat information and to validate Threat Assessment reports.
DoDD 8500.01E, Information Assurance, 23 April 2007, Unclassified	Summary: This directive establishes that all Department of Defense (DoD) information systems shall maintain… documented threats and vulnerabilities. It assigns responsibility to the Director, Defense Intelligence Agency (DIA), to provide finished intelligence on information assurance (IA), including Threat Assessments to the DoD components.
CJCSI 6510.01E, Information Assurance (IA) and Computer Network Defense, 12 August 2008, Unclassified	Summary: This instruction assigns responsibilities to the Director, DIA to provide Global Information Grid (GIG) Threat Assessments and to assist in conducting GIG risk assessments for DoD components.
Committee for National Security Systems (CNSS)	
CNSSD-502 National Directive on Security of National Security Systems, 16 December 2004, Unclassified	Summary: The objective of this directive is to ensure the security of National Security Systems (NSS) and that the government's capabilities for securing them are improved. It provides focus on the requirement to provide for reliable and continuing assessment of threats and vulnerabilities,

	and implementation of appropriate, effective countermeasures.
NSTISSI 1000 National Information Assurance Certification and Accreditation Process (NIACAP), April 2000, Unclassified	Summary: This instruction identifies the certification and accreditation (C&A) process for NSS and requires the System Security Authorization agreement to document the operating environment and threat for the system.
Other Federal (OMB, NIST, …)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	

Threat Assessment Standards

Title, Date, Status	**Excerpt / Summary**
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Nothing found	
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, …)	
NIST SP 800-37 Rev 1 Guide for Applying the	Summary: This guide includes a risk management framework and includes the dissemination of updated

Risk Management Framework to Federal information Systems, February 2010, Unclassified	threat and risk information to authorizing officials and information system owners.
NIST SP 800-30 Risk Management Guide for Information Technology Systems, July 2002, Unclassified	Summary: This guide describes the risk management methodology, and threat identification and analysis are a significant part of the process.
NIST SP 800-34 Rev 1, Contingency Planning Guide for Federal Information Systems, May 2010, Unclassified	Summary: This guide describes the essential components for preparing and maintaining information system contingency plans. Identifying threats is a key part of developing the contingency plan.
Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, …)	
Nothing found	

10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)
2. Necessary training
3. Licensing (if applicable)
4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute

8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:

1. Availability of threat resources–The Enterprise will need to find information about the threats affecting them and make this information available to this Capability.
2. Storage requirements–The Enterprise will need to provide storage for threat and attacker profiles.

11 Guidance Statements

This section provides Guidance Statements, which have been extracted from Section 3 (Capability Gold Standard Guidance) of this Capability document. The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the Threat Assessment Capability.

- The Enterprise shall identify, analyze, and prioritize threat information by identifying threats and threat sources, understanding the threat's capability, and determining the likelihood of the threat occurring.
- Analysis of threats and threat sources shall occur for all attacks against technical, personnel, physical, and environmental aspects of the Enterprise, including supply chain, close access technical attacks, and insider threats.
- Threat assessments shall encompass threat awareness, investigations, active operations, provocations, and deception activities.
- Threat information shall be obtained from multiple sources to create a comprehensive threat picture. Sources shall include the broader intelligence and law enforcement community; government, civilian, and commercial sources of threat; and incident, attack, IT security, and virus scanning industries.
- The Enterprise shall understand how threat assessments are handled and what resources it can rely on internally as well as externally for threat assessment information.
- If an Enterprise relies on an external Organization, the Enterprise shall identify a subset of threats that apply to local enclaves as well as at the Enterprise level.
- Internal resources for threat information shall be available at the local level within the Enterprise, such as the SSO.

- If an Enterprise is not large or does not have the manpower to stand up its own threat Organization, a formal relationship shall be established with a set of external organizations to provide the needed threat data in the appropriate form and format.
- If threat data is obtained from an external Organization, the Enterprise shall perform further analysis on applicability to its enclave/Organization.
- Analysis shall be performed on raw data received from other Community Gold Standard Capabilities to ensure the information is applicable, useful, and contributes to overall situational awareness.
- Each identified threat shall be assigned a priority.
- Threat reporting shall occur within an Enterprise.
- Organizational cooperation shall be in place between Organizations to share threat information. Threat reports shall be shared with affected Organizations and Organizations with similar threats.
- Evolving threats shall be monitored and analyzed for trends to determine capabilities of attackers.